

PRIVACY POLICY

in support of Cybertrust's Public Certification Services

version 1.2 – Date of last modification: September 11, 2007



IMPORTANT NOTICE: You must not apply for, accept or use Cybertrust's public certificate services before reading and agreeing to this Privacy Policy and the Cybertrust Certification Practice Statement (hereinafter "CPS"), a current version of which is located at <http://cybertrust.omniroot.com/repository.cfm>. This Privacy Policy is ancillary to the CPS and does, as such, not replace (in whole or in part) the CPS, which ultimately controls the provision of Cybertrust's public certification services.

INTRODUCTION

This Privacy Policy (hereinafter "Policy") applies to Cybertrust's Public Certification Services. Except where expressly set forth otherwise in the Policy, references to "Cybertrust" shall be deemed references to Cybertrust Belgium NV, BTW BE 0.455.138.450 RPR Leuven, a Belgian corporation that, in its capacity as Public Certification Authority, controls and operates the Cybertrust Public Certification Services in respect of which this Policy applies and that, at the date of this Policy, forms part of the Cybertrust group of companies. This Policy serves to describe what types of personally identifiable information Cybertrust collects and how Cybertrust uses such information in connection with its Public Certification Services Cybertrust (either by itself or through an affiliate or agent).

1. TYPE OF PERSONAL INFORMATION THAT MAY BE COLLECTED

1.1. In connection with its Public Certification Services Cybertrust collects, in general, the following types of personal information:

- (i) information provided by a certificate applicant and/or subscriber (such as, for example, name, organization name, physical and email address, contact details, birth date, gender, personal registration number, social security number, professional qualification and/or function title);
- (ii) information regarding the use of Cybertrust's web site(s) by a certificate applicant and/or subscriber;
- (iii) electronic mail communication from a certificate applicant and/or subscriber;
- (iv) information from other sources rightfully received or obtained.

1.2. Cybertrust may collect personal information both off-line and on-line. Cybertrust may use one or more web sites in connection with its Public Certification Services. Any such site is primarily intended for use by commercial companies or businesses and their representatives. It provides a way for commercial professionals to obtain information about, and to access Cybertrust products and services on-line. It is not a site intended for the use of persons under the age of 18 or persons that otherwise do not have the legal capacity to enter into binding agreements.

1.3. Cybertrust collects information as proportional to its intended use. By way of an example, the type and degree of information collected may vary according to the type and class of certificate applied for as more or less stringent vetting procedures apply. Cybertrust may retain personal information for up to thirty (30) years depending on the product or service and further upon applicable law.

2. PURPOSE

2.1. Notwithstanding any other collection and/or usage practices that may be detailed herein, Cybertrust collects and uses personal information for one or more of the following purposes:

- (i) to administer, bill and account for Cybertrust products and/or services applied for and/or purchased;
- (ii) to verify and/or proof information provided during the certificate application process (such as, information regarding an applicant's identity);
- (iii) to provision certificates and certificate lifecycle management services;
- (iv) to provide technical and/or administrative information and/or support;
- (v) as required by applicable law;
- (vi) to communicate about Cybertrust products and/or services;
- (vii) for statistical, historical or scientific purposes (such as, for example, performing analyses of user behavior in order to measure interest in and use of the various areas of the Cybertrust site(s)).

2.2. Where Cybertrust collects personal information for statistical, historical or scientific purposes, Cybertrust will use reasonable means to aggregate the personal information or make such information anonymous prior to public use so that the personal information cannot be accessed as such.

3. APPLICABILITY

3.1. This Policy applies to the extent Cybertrust collects and uses personal information in connection with its Public Certification Services including, by way of an example, certificate lifecycle management services related to the following types of certificates:

Certificate Type / Class
SureCredential 2 certificate

SureCredential 2PRO certificate
SureCredential 3 certificate
SureCredential 3PRO certificate
SureServer certificate
SureServer EV certificate
SureServer EDU certificate
SureCodeSign certificate
OmniRoot certificate
Cybertrust Administrative certificates

3.2. This policy applies in addition to, and not in lieu of, any other privacy policy that Cybertrust may maintain. To the extent of any conflict, the provisions of this Policy shall prevail but only as it concerns personal information collected and/or used by Cybertrust in connection with its Public Certification Services.

4. SECURITY AND DATA INTEGRITY

4.1. Cybertrust takes reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction. More information on the associated technical and organizational precautionary measures are described in this Policy and or Cybertrust's most recent CPS which is currently located at <http://cybertrust.omniroot.com/repository.cfm>.

5. LOGGED FILES AND COOKIES

5.1. On some pages of the Cybertrust website used in connection with Cybertrust's Public Certification Services, one may be able to order products and/or services, make requests, and register to receive materials. Many items may not be accessible without registration. The types of personal information collected at these pages are logged files and cookies. IP addresses and browser types are logged for systems administration purposes and these logs will be analyzed to constantly improve the value of the materials available on the web site. IP addresses are as such not linked to anything personally identifiable. This means that a user's session will be tracked, but the user will be anonymous. A cookie is set that is in no way related to any personally identifiable information. A cookie is set to facilitate future usage of the web site. The site(s) also use cookies that track server-side data, and these cookies are terminated once the user closes their browser. If a user rejects the cookie, they may still use the Cybertrust web site. Cybertrust does not use cookies to track and target Cybertrust users in any particular way, nor do we collect this information for such purpose.

6. AGENTS

6.1. Cybertrust may by itself or through an agent (such as, for example, an outside payment gateway and credit card processing company) collect and transmit personally identifiable information for the purposes of (i) billing and/or accounting for products and services; (ii) performing business administration; (iii) marketing; (iv) customer services; (v) performing other business functions. To the extent permitted by applicable law, such agents will not be permitted to collect and/or use personal information for any purposes other than to perform their assigned functions.

7. TRANSFERS

7.1. In connection with Cybertrust's Public Certification Services, personal information regarding data subjects (such as certificate applicants and subscribers) may be transferred to and from jurisdictions that are subject to the Directive 95/46/EC of the European Parliament on "The protection of individuals with regard to the processing of personal data and on the free movement of such data" and any secondary legislation thereof (including, legislation and regulations implementing the aforementioned Directive and secondary legislation in a national jurisdiction) ("EU Personal Data

PRIVACY POLICY

in support of Cybertrust's Public Certification Services

version 1.2 – Date of last modification: September 11, 2007



Processing Legislation). Cybertrust requires the intended recipient data handler to provide such adequate privacy protection as required by the EU Personal Data Processing Legislation, including, where applicable, adherence to the so-called Safe Harbor certification, to the extent Cybertrust's transfer of such personal information would be subject to the EU Personal Data Processing Legislation in a manner that would require Cybertrust to do so.

- 7.2. Certain business transactions may occur pursuant to which a person or entity acquires all or substantially all of Cybertrust's business, stock or assets pursuant to a merger, asset sale or similar transaction. As a result of or in connection with such transaction, Cybertrust may transfer any personal information and/or assign any policies and service agreements to the acquiring party.

8. LINK TO THIRD PARTY SITES

- 8.1. Cybertrust may provide links in portions of its web site that will let one leave the Cybertrust site. The linked sites are not under the control of Cybertrust and Cybertrust is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Cybertrust is not responsible for any transmission received from any linked site. Cybertrust is providing these links only as a convenience and the inclusion of any link does not imply endorsement by Cybertrust of the site or its content. This Policy does not extend to such sites and Cybertrust makes no representations regarding the protection of personal data offered on those sites. One should consult such other site's policies and disclaimers prior to using such site (including, without limitation, providing personal information).

9. DISCLOSURES

- 9.1. Cybertrust may be required (and accordingly reserves the right) to disclose personal information (i) as required by law or applicable regulations; (ii) pursuant to or to comply with a judicial proceeding, subpoena, court order, or legal process which may be without notice to the data subject; (iii) as required by Cybertrust's other legal obligations or to defend Cybertrust's (or Cybertrust's affiliated entities and agents') interests.

10. OPT-OUT

- 10.1. Should Cybertrust intend to use and disclose to a third party a data subject's personal information for any purpose other than described herein or otherwise not previously authorized by the data subject, Cybertrust will afford the data subject an opportunity to confirm its consent or to withhold its consent prior to Cybertrust actual usage and disclosure. The foregoing provision applies to the extent required by applicable law.

11. POLICY ACCEPTANCE AND UPDATES

- 11.1. By providing personal information to Cybertrust, the providing party signifies agreement to the terms of this Policy.
- 11.2. This Policy as well as other policies, statements, agreements, information and materials (collectively "Materials") related to or associated with Cybertrust's certification services and the provision thereof may be updated, revised, supplemented or replaced from time to time by Cybertrust in its sole discretion and without prior notice. A data subject is responsible to monitor and maintain awareness of any such changes to the Materials. Unless a later date is indicated by Cybertrust, Materials become effective upon the date such Materials are posted by Cybertrust under the Cybertrust Repository currently located at <http://cybertrust.omniroot.com/repository.cfm>.

12. ACCESS AND REMEDIATION

- 12.1. Any data subject (such as a certificate applicant or subscriber) from whom Cybertrust collected and holds personal information can contact Cybertrust to review and correct their respective personal information where that information would be inaccurate, to the extent required by applicable law. To that end, a data subject should contact Cybertrust at Cybertrust Legal Department (EMEA) – Philipssite 5 – B-3001 Leuven – Belgium. Cybertrust may limit access rights as permitted by applicable law.
- 12.2. If a data subject (such as a certificate applicant or a subscriber) has good reason to believe that Cybertrust violated this Policy, that data subject is invited to contact Cybertrust immediately at Cybertrust Legal Department (EMEA) – Philipssite 5 – B-3001 Leuven – Belgium. Cybertrust uses the BBBOnline Privacy Program as a method for providing consumers with access to an independent, dispute resolution mechanism.

13. GOVERNING LAW

- 13.1. This Policy is construed, interpreted and enforced in accordance with the laws of Belgium, exclusive of any choice of law rules. Any and all disputes, claims or litigation arising from or related in any way to this Policy shall be resolved by the courts located in Brussels, Belgium. Any party calling upon this Policy agrees to waive any objections against and agrees to submit to the aforementioned jurisdiction.